Ilann M. Maazel
Matthew D. Brinckerhoff
Emery Celli Brinckerhoff & Abady LLP
75 Rockefeller Plaza, 20th Floor
New York, New York 10019
Telephone: (212) 763-5000
Facsimile: (212) 763-5001
Attorneys for Plaintiffs

IN THE UNITED STATES DISTRICT COURT
FOR THE NORTHERN DISTRICT OF CALIFORNIA

IN RE NATIONAL SECURITY AGENCY TELECOMMUNICATIONS RECORDS LITIGATION This Document Relates to: VIRGINIA SHUBERT, NOHA ARAFA, SARAH DRANOFF and HILARY BOTEIN, individually and on behalf of all others similarly situated, Plaintiffs, -against - GEORGE W. BUSH, MICHAEL V. HAYDEN, KEITH B. ALEXANDER, ALBERTO GONZALES, JOHN ASHCROFT, UNITED STATES OF AMERICA, and JOHN/JANE DOES #1-100 (07-693)	MDL Dkt. No. 06-1791-VRW **AMENDED CLASS ACTION COMPLAINT/DEMAND FOR JURY TRIAL**

Plaintiffs Virginia Shubert, Noha Arafa, Sarah Dranoff, and Hilary Botein, by their attorneys Emery Celli Brinckerhoff & Abady LLP, for their Amended Complaint, allege as follows:

Dockets.Justia.

PRELIMINARY STATEMENT

1. This class action challenges the Bush Administration's secret spying program pursuant to which, on information and belief, virtually every telephone, internet and/or email communication that has been sent from or received within the United States since 2001 has been (and continues to be) searched, seized, intercepted, and subjected to surveillance without a warrant, court order or any other lawful authorization in violation of the Foreign Intelligence Surveillance Act of 1979, 50 U.S.C. § 1810.

2. Without the approval of Congress, without the approval of any court, and without notice to the American people, the current President of the United States authorized a secret program to spy upon millions of innocent Americans, including the named plaintiffs. This program (the "Spying Program") – intercepting, searching, seizing, and subjecting to surveillance the content of personal phone conversations and email of millions of unsuspecting, innocent Americans – is illegal. It violates the plain terms of federal statutes that makes such conduct a crime.[1] It violates the Constitution. It violates the most basic principles of separation of powers.

3. The government's spy agency, the National Security Agency ("NSA"), spied upon Americans at home. It spied upon Americans at work. And it is spying today, and will continue to spy on millions of innocent, unsuspecting Americans, unless stopped by a federal court.

4. The American people deserve better. The American people should not be subjected to a illegal, covert, dragnet spying operation by their own government. This class

---

[1] *E.g.* The Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* ("FISA"); the Wiretap Act 18 U.S.C. § 2510 *et seq.*; the Stored Communications Act, 18 U.S.C. § 2701 *et seq.* ("SCA").

action is brought on behalf of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant, court order, or other lawful authorization since September 12, 2001.[2] It primarily seeks liquidated damages under the Federal Intelligence Surveillance Act 50 U.S.C. § 1810 *et. seq.* ("FISA"), which authorizes civil actions for violations of FISA.

PARTIES

5. Plaintiff Virginia Shubert is an American citizen who resides and works in Brooklyn, New York. Ms. Shubert regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Shubert, for example, frequently calls and sends emails to the United Kingdom, France and Italy and has made similar communications as a part of her work. Since September 12, 2001, Ms. Shubert has been and continues to be a customer of AT&T, which, on information and belief, participated and participates in the Spying Program. Ms. Shubert, like so many millions of Americans, has been surveilled without a warrant pursuant to the illegal Spying Program.

6. Plaintiff Noha Arafa is an American citizen who resides and works in Brooklyn, New York. She regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Arafa, for example, frequently calls and sends emails to family and friends in Egypt from her home, and has made telephone calls abroad as a part of her work. Since September 12, 2001, Ms. Dranoff has been and continues to be a customer of a customer of AT&T, which, on information and belief, participated and participates in the Spying

---

[2] "United States persons" and "electronic surveillance" are both defined terms set forth in FISA. 50 U.S.C. § 1801.

Program. Ms. Arafa, like so many millions of Americans, has been surveilled without a warrant pursuant to the illegal Spying Program.

7. Plaintiff Sarah Dranoff is an American citizen who resides and works in Brooklyn, New York. Ms. Dranoff regularly makes phone calls and sends email both within the United States, and outside the United States. Ms. Dranoff for example, calls the Netherlands and sends emails to the Netherlands and Norway from her home. Since September 12, 2001, Ms. Dranoff has been a customer of Verizon and of AT&T, which, on information and belief, participated and participates in the Spying Program. Ms. Dranoff, like so many millions of Americans, has been surveilled without a warrant pursuant to the illegal Spying Program.

8. Plaintiff Hilary Botein is an American citizen who resides and works in Brooklyn, New York. Ms. Botein makes phone calls and sends email both within the United States, and outside the United States. Since September 12, 2001, Ms. Botein has been a customer of Verizon which, on information and belief, participated and participates in the Spying Program. Ms. Botein, like so many millions of Americans, has been surveilled without a warrant pursuant to the illegal Spying Program.

9. Defendant George W. Bush is the current President of the United States. Mr. Bush authorized the illegal Spying Program.

10. Defendant Lieutenant General Michael V. Hayden is the former Director of the NSA. While Director, defendant Hayden had ultimate authority for supervising and implementing all operations and functions of the NSA, including the illegal Spying Program. Defendants Hayden also apparently approved the illegal initiation of the Spying Program.

11. Defendant Lieutenant General Keith B. Alexander is the current Director of the NSA. Defendant Alexander has ultimate authority for supervising and implementing all operations and functions of the NSA, including the illegal Spying Program.

12. Defendant John Ashcroft is the former Attorney General of the United States. Although, according to some published reports, defendant Ashcroft had reservations concerning the Spying Program, Mr. Ashcroft ultimately approved and authorized the Spying Program.

13. Defendant Alberto Gonzales is the current Attorney General of the United States. Defendant Gonzales approved and authorized the Spying Program and has consistently defended the program before Congress and in other public fora.

14. Defendant Bush and the other individual defendants work for the government of the United States of America, which has conducted and continues to conduct the illegal Spying Program.

15. At all times relevant hereto, defendants John and Jane Does #1-100 (the "Doe defendants"), whose actual names plaintiff has been unable to ascertain notwithstanding reasonable efforts to do so, but who are sued herein by the fictitious designation "John Doe" and "Jane Doe," were agents and employees of the NSA, Department of Homeland Security, Department of Justice, the White House, or other government agencies, acting in the capacity of agents, servants, and employees of the United States government, and within the scope of their employment as such, who conducted, authorized, and/or participated in the Spying Program.

JURISDICTION AND VENUE

16. This action arises under the Fourth Amendment to the United States Constitution, the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.*, the Wiretap Act 18 U.S.C. § 2510 *et seq.*; and the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*

17. The jurisdiction of this Court is predicated upon 28 U.S.C. §§ 1331, 1343(a)(4).

18. Venue is proper in this district pursuant to 28 U.S.C. § 1391(e).

JURY DEMAND

19. Plaintiffs demand trial by jury in this action.

CLASS ACTION ALLEGATIONS

20. The plaintiff class seeks (i) a judgment declaring that the Spying Program violates FISA, the Wiretap Act, the SCA, and the Fourth Amendment, (ii) an order enjoining defendants from engaging in the Spying Program, and (iii) liquidated damages as set forth in 50 U.S.C. § 1810, and 18 U.S.C. §§ 2520, 2707 to redress the extraordinary invasion of privacy caused by the Spying Program.

21. Plaintiffs sue on behalf of themselves and all other similarly situated individuals, and seek to represent a class comprised of all present and future United States persons who have been or will be subject to electronic surveillance by the National Security Agency without a search warrant, court order, or other lawful authorization since September 12, 2001.

22. The members of the class are so numerous as to render joinder impracticable.

23. The questions of law and fact common to the class include that the class members were all subject to electronic surveillance without a search warrant, court order, or any lawful authorization pursuant to the Spying Program; all have the common right under FISA, the Wiretap Act, and the SCA to be free from electronic surveillance absent a search warrant or court order, the common right under FISA, the Wiretap Act, and the SCA to liquidated damages for violations of those rights, and the common right under the Fourth Amendment to be free from electronic surveillance absent a search warrant or court order. Defendants' electronic surveillance without a search warrant, court order, or any lawful authorization violated those rights.

24. The named plaintiffs are adequate representatives of the class. The violations of law alleged by the named plaintiffs stem from the same course of conduct by defendants – failure to seek a search warrant, court order, or any other lawful authorization before conducting electronic surveillance – that violated and continue to violate the rights of members of the class; the legal theory under which the named plaintiffs seek relief is the same or similar to that on which the class will rely. In addition, the harms suffered by the named plaintiffs are typical of the harms suffered by the class members, especially given the common calculation of liquidated damages.

25. The named plaintiffs have the requisite personal interest in the outcome of this action and will fairly and adequately protect the interests of the class. The named plaintiffs are represented by Emery Celli Brinckerhoff & Abady LLP ("ECBA"). Counsel has the

resources, expertise and experience to prosecute this action. Counsel for the plaintiffs knows of no conflicts among members of the class or between ECBA and members of the class.

26. A class action is superior to other available methods for the fair and efficient adjudication of this controversy because: (i) the prosecution of millions of separate actions would be inefficient and wasteful of legal resources; (ii) the members of the class are scattered throughout the United States and are not likely to be able to vindicate and enforce their statutory and constitutional rights unless this action is maintained as a class action; (iii) the issues raised can be more fairly and efficiently resolved in the context of a single class action than piecemeal in many separate actions; (iv) the resolution of litigation in a single forum will avoid the danger and resultant confusion of possible inconsistent determinations; (v) the prosecution of separate actions would create the risk of inconsistent or varying adjudications with respect to individuals pursuing claims against defendants which would establish incompatible standards of conduct for defendants; and (vi) questions of law and/or fact common to members of the class predominate over any question that affects individual members.

FACTUAL ALLEGATIONS

Classwide Allegations

Legal Framework

27. The Fourth Amendment provides that "[t]he right of the people to be secure in their persons, houses, papers, and effects, against unreasonable searches and seizures, shall not be violated, and no Warrants shall issue, but upon probable cause, supported by Oath or

affirmation, and particularly describing the place to be searched, and the persons or things to be seized."

28. Congress has enacted two statutes that together supply "the *exclusive means* by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added). The first is the Electronic Communications Privacy Act ("ECPA"), which includes the Wiretap Act, 18 U.S.C. § 2510 *et seq.*, and the Stored Communications Act, 18 U.S.C. § 2701 *et seq.*, and the second is the Foreign Intelligence Surveillance Act, 50 U.S.C. § 1801 *et seq.* ("FISA").

The ECPA

29. Congress first enacted the predecessor to the ECPA (commonly referred to as Title III) in response to the U.S. Supreme Court's recognition, in *Katz v. United States*, 389 U.S. 347 (1967), that individuals have a constitutionally protected privacy interest in the content of their telephone calls. Through Title III and then the ECPA, Congress created a statutory framework to govern the surveillance of wire and oral communications in law enforcement investigations.

30. The ECPA authorizes the government to intercept wire, oral, or electronic communications in investigations of certain enumerated criminal offenses, *see* 18 U.S.C. § 2516, with prior judicial approval, *see id.* § 2518.

31. In order to obtain a court order authorizing the interception of a wire, oral, or electronic communication, the government must demonstrate that "there is probable cause for belief that an individual is committing, has committed, or is about to commit" one of the enumerated criminal offenses. *Id.* § 2518(3)(a).

32. It must also demonstrate, among other things, that "there is probable cause for belief that particular communications concerning [the enumerated] offense will be obtained through [the] interception," *id.* § 2518(3)(b), and that "normal investigative procedures have been tried and have failed or reasonably appear to be unlikely to succeed if tried or to be too dangerous," *id.* § 2518(3)(c).

33. The ECPA specifies civil and criminal penalties for surveillance that is not authorized. *See id.* §§ 2511, 2520, 2701, 2707.

Foreign Intelligence Surveillance Act

34. The government has one and only one other legal avenue to engage in electronic surveillance: the Foreign Intelligence Surveillance Act.

35. In 1978, Congress enacted FISA to govern the use of electronic surveillance against foreign powers and their agents inside the United States. The statute created the Foreign Intelligence Surveillance Court, a court composed of seven (now eleven) federal district court judges, and empowered this court to grant or deny government applications for electronic surveillance orders in foreign intelligence investigations. *See* 50 U.S.C. § 1803(a). Congress enacted FISA after the U.S. Supreme Court held, in *United States v. United States District Court for the Eastern District of Michigan,* 407 U.S. 297 (1972), that the Fourth Amendment does not permit warrantless surveillance in intelligence investigations of domestic security threats. FISA was a response to that decision and to the Report of the Senate Select Committee to Study Government Operations with Respect to Intelligence Activities, S.Rep. No. 94-755, 94th Cong., 2d Sess. (1976) ("Church Committee Report"), which found that the

executive had engaged in warrantless wiretapping of numerous United States citizens – including journalists, activists, and Congressmen – who posed no threat to the nation's security and who were not suspected of any criminal offense. The Church Committee Report warned that "[u]nless new and tighter controls are established by legislation, domestic intelligence activities threaten to undermine our democratic society and fundamentally alter its nature."

36. When Congress enacted FISA, it provided that the procedures set out therein "shall be the *exclusive means* by which electronic surveillance . . . and the interception of domestic wire, oral, and electronic communications may be conducted." 18 U.S.C. § 2511(2)(f) (emphasis added).

37. FISA provides that no one may engage in electronic surveillance "except as authorized by statute," *id.* § 1809(a)(1).

38. FISA specifies civil and criminal penalties for electronic surveillance undertaken without statutory authority, *see id.* §§ 1809 & 1810.

39. The Senate Judiciary Committee explained that "[t]he basis for this legislation is the understanding – concurred in by the Attorney General – that even if the President has an 'inherent' Constitutional power to authorize warrantless surveillance for foreign intelligence purposes, Congress has the power to regulate the exercise of this authority by legislating a reasonable warrant procedure governing foreign intelligence surveillance." S. Rep. 95-604(I), reprinted at 1978 U.S.C.C.A.N. at 3917. The Committee further explained that the legislation was meant to "spell out that the executive cannot engage in electronic surveillance within the United States without a prior Judicial warrant." *Id.* at 3906.

40. FISA defines "electronic surveillance" to include:

a. "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire or radio communication sent by or intended to be received by a particular, known United States person who is in the United States, if the contents are acquired by intentionally targeting that United States person, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes";

b. "the acquisition by an electronic, mechanical, or other surveillance device of the contents of any wire communication to or from a person in the United States, without the consent of any party thereto, if such acquisition occurs in the United States . . .";

c. "the intentional acquisition by an electronic, mechanical, or other surveillance device of the contents of any radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes, and if both the sender and all intended recipients are located within the United States"; and

d. "the installation or use of an electronic, mechanical, or other surveillance device in the United States for monitoring to acquire information, other than from a wire or radio communication, under circumstances in which a person has a reasonable expectation of privacy and a warrant would be required for law enforcement purposes." 50 U.S.C. § 1801(f).

41. FISA defines "contents" to include "any information concerning the identity of the parties to such communication or the existence, substance, purport, or meaning of that communication." 50 U.S.C. § 1801(n).

42. FISA defines "United States person" to include United States citizens and lawful permanent residents. *Id.* § 1801(d).

43. In order to obtain an order from the FISA Court authorizing electronic surveillance, the government must demonstrate, among other things, probable cause to believe that "the target of the electronic surveillance is a foreign power or an agent of a foreign power" and that "each of the facilities or places at which the electronic surveillance is directed is being used, or is about to be used, by a foreign power or an agent of a foreign power." *Id.* § 1805(a)(3).

44. While FISA generally prohibits surveillance without prior judicial authorization, it includes a provision that allows for warrantless surveillance in "emergency situation[s]." Where an emergency situation exists and "the factual basis for issuance of an order under this subchapter to approve such surveillance exists," the statute permits the Attorney General to authorize warrantless surveillance "if a judge having jurisdiction under section 1803 of this title is informed by the Attorney General or his designee at the time of such authorization that the decision has been made to employ emergency electronic surveillance and if an application in accordance with this subchapter is made to that judge as soon as practicable, but not more than 72 hours after the Attorney General authorizes such surveillance." *Id.* § 1805(f).

45. FISA also permits electronic surveillance without a court order for fifteen days after a formal declaration of war. *Id.* § 1811 ("Notwithstanding any other law, the President, through the Attorney General, may authorize electronic surveillance without a court order under this subchapter to acquire foreign intelligence information for a period not to exceed fifteen calendar days following a declaration of war by the Congress.").

46. FISA requires the Attorney General to report to the House and Senate Intelligence Committees twice a year regarding "all electronic surveillance" authorized under FISA. *Id.* § 1808(a). Statistics released annually by the Justice Department indicate that, between

1978 and 2004, the government submitted almost 19,000 surveillance applications to the FISA Court. The FISC denied four of these applications; granted approximately 180 applications with modifications; and granted the remainder without modifications.

The Spying Program

47. Until December 2005, even the existence of the Spying Program was unknown to Congress and to the American people.

48. To the contrary, in a speech on June 9, 2005, President Bush stated: "*Law enforcement officers need a federal judge's permission to wiretap a foreign terrorist's phone, a federal judge's permission to track his calls, or a federal judge's permission to search his property. Officers must meet strict standards to use any of these tools.* And these standards are fully consistent with the Constitution of the U.S." (Emphasis supplied.)[3]

49. Although it is true that federal law requires law enforcement officers to get permission from a federal judge to wiretap, track, or search, the President secretly authorized a Spying Program that did none of those things.

50. As revealed in *The New York Times* in December 2005, and as subsequently revealed, *inter alia*, by published press reports, whistleblowers, insiders within the United States government, and (after initial equivocation) President Bush himself, in the fall of 2001 the NSA launched a secret electronic surveillance program to intercept, search and seize, without prior judicial authorization, the telephone and internet communications of people inside the United States.

---

[3]*See* http://www.whitehouse.gov/news/releases/2005/06/20050609-2.html

51. President Bush approved the Spying Program.

52. President Bush reauthorized the Spying Program more than 30 times.

53. Under the Spying Program, the NSA engages in "electronic surveillance" as defined by FISA.

54. Under the Spying Program, the NSA engages in "interception" of both "wire communication[s]" and "electronic communication[s]" as defined in the Wiretap Act. 18 U.S.C. § 2510.

55. Under the Spying Program, the NSA intentionally accesses electronic communications without authorization and/or exceeds authorization to access electronic communications that are maintained in "electronic storage" as defined by the SCA.

56. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance international telephone communications of people inside the United States, including citizens and lawful permanent residents, including plaintiffs.

57. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance international internet communications, including email, of people inside the United States, including citizens and lawful permanent residents, including plaintiffs.

58. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance domestic telephone communications and call data of people inside the United States, including citizens and lawful permanent residents.

59. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance domestic internet communications, including email, of people inside the United States, including citizens and lawful permanent residents.

60. Under the Spying Program, the NSA has intercepted, subjected to electronic surveillance, and searched and seized millions of international telephone and internet communications (hereinafter collectively "communications") of people inside the United States, including citizens and lawful permanent residents, including plaintiffs.

61. Under the Spying Program, the NSA has intercepted, searched and seized, and subjected to electronic surveillance purely domestic communications, that is, communications among people all of whom are inside the United States.

62. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without probable cause to believe that the surveillance targets have committed or are about to commit any crime.

63. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without probable cause to believe that the surveillance targets are foreign powers or agents thereof.

64. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without reasonable suspicion or any reason whatsoever to believe that the surveillance targets either have committed or are about to commit any crime or are foreign powers or agents thereof.

65. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without obtaining specific authorization for each interception from the President.

66. Under the Spying Program, the NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of people inside the United States without obtaining specific authorization for each interception from the Attorney General.

67. Under the Spying Program, NSA shift supervisors are authorized to approve NSA employees' requests to intercept, search and seize, and subject to electronic surveillance the communications of people inside the United States.

68. Under the Spying Program, the NSA uses NSA-controlled satellite dishes to intercept, search and seize, and subject to electronic surveillance communications that are transmitted via satellite.

69. Some of these NSA-controlled satellite dishes are located within the United States.

70. The NSA also works with telecommunications companies to intercept, search and seize, and subject to electronic surveillance communications that pass through switches controlled by these companies.

71. These switches, which are located inside the United States, serve as primary gateways for communications going into and out of the United States. The switches connect to transoceanic fiber optic cables that transmit communications to other countries.

72. The NSA also works with internet providers and telecommunications companies to intercept, search and seize, and subject to electronic surveillance communications, including email, telephone and internet including email.

73. As part of the Spying Program, the NSA uses government computers to search for keywords and analyze patterns in millions of communications at any given time.

74. If, for example, such keywords included "jihad," "Iraq," "Bush is a criminal," or whatever words or phrases the United States government deems of interest, then, pursuant to the Spying Program, persons at the NSA may target those Americans for even further interception, search and seizure, and electronic surveillance.

75. The NSA also intercepts, searches and seizes, and subjects to electronic surveillance international communications between persons in the United States and persons outside the United States.

76. The NSA intercepts, searches and seizes, and subjects to electronic surveillance hundreds of millions of internet and telephone communications.

77. The NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of millions of innocent, law-abiding Americans who have no connection whatsoever to terrorism.

78. The NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of Americans in their homes, including private phone conversations, private email, and private internet use.

79. The NSA intercepts, searches and seizes, and subjects to electronic surveillance the communications of Americans at their place of work, including private phone conversations, private email, and private internet use.

80. Under the Spying Program, hundreds of millions of phone, email, and internet communications by United States persons have been intercepted, searched and seized, and subjected to electronic surveillance by government spy computers at the NSA.

81. On information and belief, the NSA also intercepts, searches and seizes, and subjects to electronic surveillance purely domestic communications.

82. Under the Spying Program, the NSA does not obtain judicial review before or after intercepting, searching and seizing, and subjecting to electronic surveillance the communications of people inside the United States.

83. Under the Spying Program, the NSA does not obtain a search warrant before or after intercepting, searching and seizing, and subjecting to electronic surveillance the communications of people inside the United States.

84. Under the Spying Program, the NSA does not obtain a court order before or after intercepting, searching and seizing, and subjecting to electronic surveillance the communications of people inside the United States.

85. Under the Spying Program, the NSA does not obtain any lawful authorization before or after intercepting, searching and seizing, and subjecting to electronic surveillance the communications of people inside the United States.

86. On information and belief, pursuant to the secret Spying Program, the NSA has intercepted, searched and seized, and subjected to electronic surveillance private

communications between Americans and their husbands, wives, children, parents, friends, pastors, doctors, lawyers, accountants, and others.

87. Each of the named plaintiffs were, pursuant to the Spying Program, subject to the unlawful interception, search and seizure, and electronic surveillance of the contents of their phone and internet communications.

88. Prior to its initiation, defendants never advocated that Congress enact a bill authorizing the illegal Spying Program.

89. Prior to its initiation, defendants never sought authorization from the FISA Court to conduct the Spying Program.

90. Prior to its initiation, defendants never sought authorization from any Article III Court to conduct the Spying Program.

91. Defendants were, or should have been, well aware that the Spying Program was a clear violation of the law.

92. Defendants were, or should have been, well aware that the Spying Program is a federal crime.

93. The Spying Program was so blatantly illegal that, according to uncontroverted press reports, even the Acting Attorney General refused to approve the program, forcing defendants to send the White House Counsel and Chief of Staff to seek approval from Attorney General Ashcroft from his hospital bed.

94. The Spying Program was so blatantly illegal that at least a dozen government officials with knowledge of the Program felt compelled as whistleblowers to report

defendants' illegal conduct to *The New York Times*, notwithstanding substantial risks to their employment and potentially to their liberty.

95. After the revelations to *The New York Times*, defendant Bush authorized a criminal investigation into the whistleblowing activity.

96. To plaintiffs' knowledge, however, defendants have failed to open any criminal investigation into the Spying Program itself.

FIRST CAUSE OF ACTION

Foreign Intelligence Surveillance Act, 50 U.S.C. § 1810

97. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

98. Plaintiffs are "aggrieved person[s]" as defined in 50 U.S.C. § 1810, are not foreign powers or agents of a foreign power, and were subjected to electronic surveillance conducted or authorized by defendants pursuant to the Spying Program in violation of 50 U.S.C. § 1809.

99. Defendants are "person[s]" within 50 U.S.C. § 1801(m).

100. Plaintiffs are entitled to the damages set forth in 50 U.S.C. § 1810.

SECOND CAUSE OF ACTION

Wiretap Act, 18 U.S.C. § 2510

101. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

102. Plaintiffs are "aggrieved person[s]" as defined in 18 U.S.C. § 2510.

103. The contents of plaintiffs' wire and electronic communications were intercepted by defendants pursuant to the Spying Program in violation of 18 U.S.C. § 2511.

104. Plaintiffs are entitled to the damages set forth in 18 U.S.C. § 2520.

THIRD CAUSE OF ACTION

Stored Communications Act, 18 U.S.C. § 2701

105. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

106. Plaintiffs are "aggrieved" within 18 U.S.C. § 2707(a).

107. Defendants intentionally accessed plaintiffs' stored communications without authorization pursuant to the Spying Program in violation of 18 U.S.C. § 2701.

108. Plaintiffs are entitled to the damages set forth in 18 U.S.C. § 2707(c).

FOURTH CAUSE OF ACTION

Bivens/Fourth Amendment

109. Plaintiffs repeat and reallege the foregoing paragraphs as if the same were fully set forth at length herein.

110. By conducting, authorizing, and/or participating in the electronic surveillance of plaintiffs, and by searching and seizing the contents of plaintiffs' communications without reasonable suspicion or probable cause, and failing to prevent their fellow government officers from engaging in this unconstitutional conduct, defendants deprived plaintiffs of rights, remedies, privileges, and immunities guaranteed under the Fourth Amendment of the United States Constitution.

111. In addition, defendants conspired among themselves to deprive plaintiffs of their Fourth Amendment rights, and took numerous overt steps in furtherance of such conspiracy, as set forth above.

112. As a direct and proximate result of the misconduct and abuse of authority detailed above, plaintiffs sustained a shocking loss of privacy, and the damages hereinbefore alleged.

WHEREFORE, plaintiffs respectfully seek:

(A) an order certifying this action as a class action pursuant to Fed. R. Civ. P. 23(b) for the plaintiff class described herein and naming plaintiffs as the class representatives;

(B) a judgment declaring that defendants' Spying Program violates FISA, the Wiretap Act, SCA, and the Fourth Amendment, and permanently enjoining the Spying Program;

(C) an award of liquidated and/or compensatory damages to the named plaintiffs and members of the class in an amount to be determined at trial;

(D) an award of punitive damages to the named plaintiffs and members of the class against the individual defendants in an amount to be determined at trial;

(E) an award of reasonable attorneys' fees, costs, and disbursements, pursuant to 50 U.S.C. § 1810, 18 U.S.C. § 2520, 18 U.S.C. § 2707, and 28 U.S.C. § 2412.

(F) a grant of such other and further relief as this Court shall find just and proper.

Dated: May 11, 2007
New York, New York

EMERY CELLI BRINCKERHOFF
& ABADY LLP

By: ______________________
Ilann M. Maazel (IM-5724)
Matthew D. Brinckerhoff (MB-3552)

75 Rockefeller Plaza, 20th Floor
New York, N.Y. 10019
(212) 763-5000

Attorneys for Plaintiffs